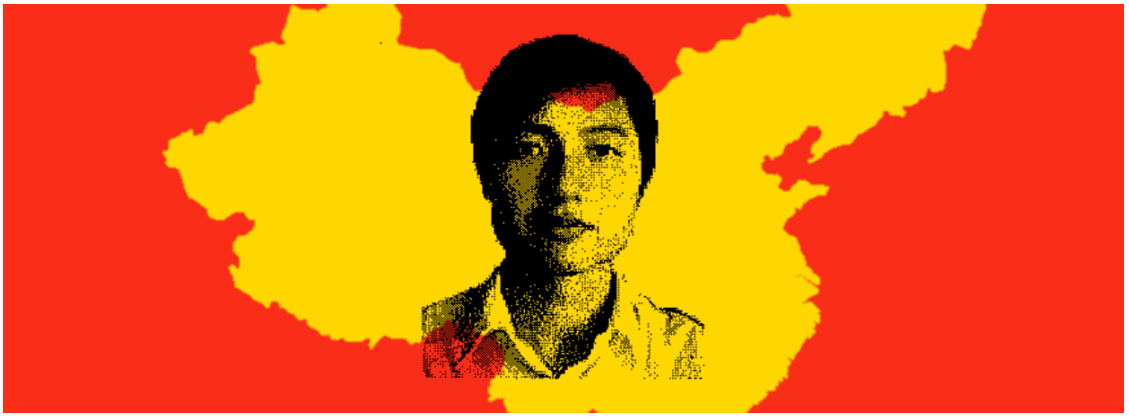
US Arrests Chinese Man Involved With Sakula Malware Used in OPM and Anthem Hacks

By Catalin Cimpanu

Published: 2017-08-26 · Archived: 2026-04-02 10:55:20 UTC

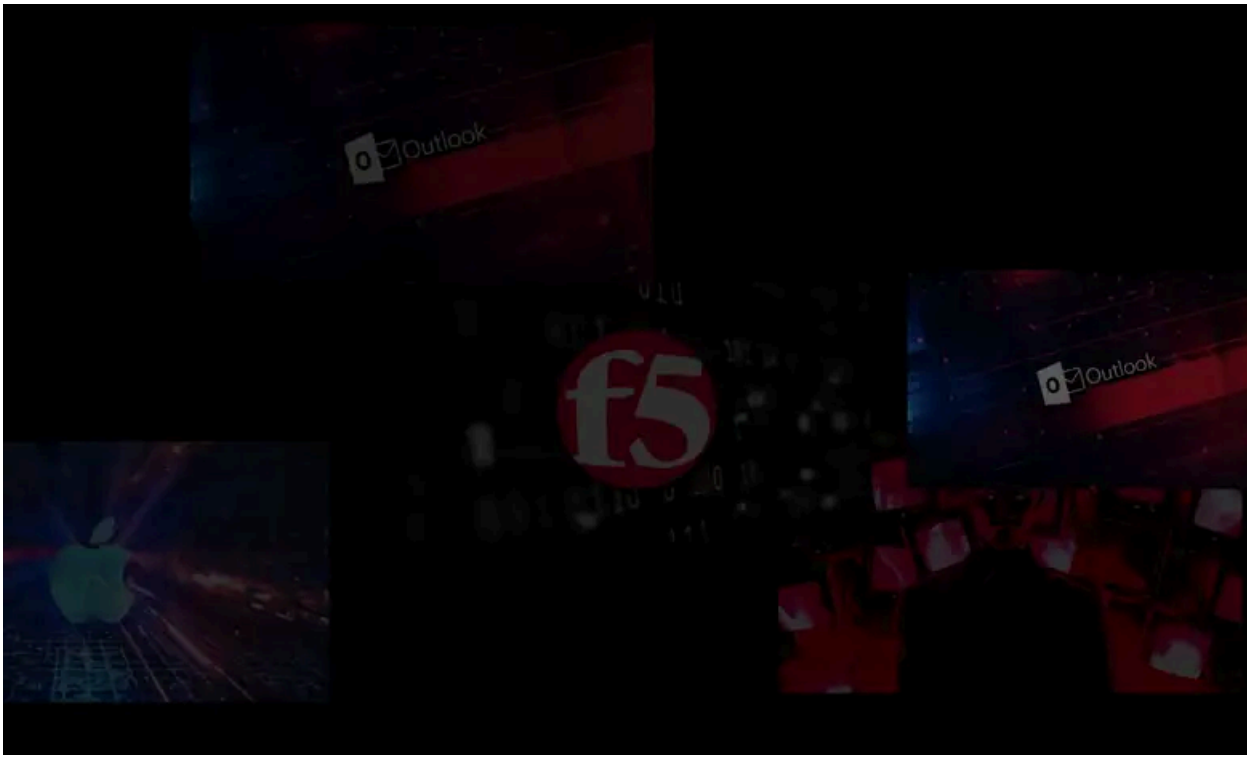


The FBI has arrested a Chinese national on accusations of distributing and infecting US companies with the Sakula malware, the same malware used in the OPM and Anthem hacks.

The suspect's name is Yu Pingan, 26, of Shanghai. US authorities arrested Yu on Monday, August 21, at the Los Angeles airport, as the suspect entered the US to attend a security conference.

Yu alleged criminal past tied to Sakula trojan

According to an official indictment, authorities accused Yu and two other unnamed co-conspirators of infecting four US companies with Sakula, a backdoor trojan.


Outlook
f5
Outlook

The US Department of Justice described Yu as a "malware broker" and charged him with the tool's distribution and four hacking charges. US authorities did not accuse Yu of creating Sakula, nor hacking OPM or Anthem.

Between 2014 and 2015, hackers stole the personal records of over 21 million government employees from the US Office of Personnel Management (OPM), and over 80 million medical records from Anthem Inc., a US company that provides health insurance, including for several government agencies.

Yu accused of using three zero-days, knowing of a fourth

US cyber-security firms have accused Chinese state hackers of carrying out the OPM and Anthem breaches. They blamed a cyber-espionage unit named Deep Panda — also known as APT19.

US authorities did not elaborate on Yu's connection to Deep Panda. Nonetheless, the indictment mentioned that Yu and his co-conspirators were in the possession of at least four zero-days — CVE-2014-0322 (affecting IE10), CVE-2012-4969 (affecting IE6), CVE-2012-4792 (affecting IE6), and an unidentified Flash Player zero-day that Yu mentioned in chat transcripts.

The hacks for which Yu stands accused all took place before the OPM and Anthem breaches. Historically, security firms have observed the Sakula trojan used in nation-state cyber-espionage campaigns exclusively.

Yu will be arraigned in court next week.

On a side note, the video below gives a basic introduction into nation-state cyber-espionage campaigns. At 27:55, security expert The Grugq provides a very simple explanation of why Chinese hackers targeted OPM and Anthem. The rest of the video also explains how the Chinese cyber apparatus works, along with similar infrastructures in Russia and the US.

Source: https://www.bleepingcomputer.com/news/security/us-arrests-chinese-man-involved-with-sakula-malware-used-in-opm-and-anthem-hacks/